IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF IOWA
CENTRAL DIVISION

JAMES A. CEDERDAHL, Plaintiff, vs. EQUIFAX INFORMATION SERVICES, LLC, Defendant.	Case No. CLASS ACTION COMPLAINT Jury Trial Demanded

Plaintiff, James A. Cederdahl, by and through his undersigned counsel, brings this action against Equifax Information Services, for violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq*., and Iowa Code Chapter 715C, *et seq*. states as follows:

PARTIES, JURISDICTION, & VENUE

1. Plaintiff James A. Cederdahl is a natural person and at all relevant times has been residing in Des Moines, Polk County, Iowa.

2. Mr. Cederdahl is, and at all relevant times was, a "consumer" as that term is defined under 15 U.S.C. 1681a(c) and Iowa Code section 715C.1(1).

3. Defendant Equifax Information Services, LLC is a limited liability company incorporated under the laws of the State of Georgia with its principal place of business located at 1550 Peachtree Street NE, Atlanta, GA and doing business in the State of Iowa.

4. Equifax is a "Consumer Reporting Agency" (CRA) as that term is defined by 15 U.S.C. 1681a.

5. Equifax is also a "Consumer Reporting Agency that Compiles and

Maintains Files on Consumers on a Nationwide Basis" as that term is defined under 15 U.S.C. 1681a(p).

6. This Court has jurisdiction over this matter pursuant to 28 U.S.C. 1331, as this case alleges a violation of federal law, specifically the Fair Credit Reporting Act, 15 U.S.C. 1681, *et seq*. (FCRA).

7. This Court has supplemental jurisdiction to hear all state law claims pursuant to 28 U.S.C. 1367.

8. Venue in this District is proper pursuant to 28 U.S.C. § 1391(b) and (c), as the Plaintiffs reside within the District, a substantial portion of the events or omissions giving rise to the claim occurred in this District, and Equifax regularly conducts business in this District.

INTRODUCTION

9. The United States Congress has found the banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system, and unfair credit reporting methods undermine the public confidence, which is essential to the continued functioning of the banking system. Congress enacted the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq. (FCRA), to insure fair and accurate credit reporting, promote efficiency in the banking system, and, as most relevant to this Complaint, protect consumer privacy. The FCRA imposes duties on the CRA's to protect consumer's sensitive personal information.

10. The FCRA protects consumers through a set of procedural protections from the material risk of harms that otherwise follow from the compromise of a consumer's sensitive personal information. Thus, through the FCRA, Congress struck a balance between the credit industry's desire to base credit decisions on accurate information, and

a consumer's substantive right to protection from damage to reputation, shame, mortification, and emotional distress that naturally follows from the compromise of a person's identity.

11. A central duty that the FCRA imposes upon CRAs is the duty to protect the consumer's privacy by guarding against inappropriate disclosure to third parties. 15 U.S.C. § 1681b codifies this duty, and permits a CRA to disclose a consumer's information only for one of a handful of exclusively defined "permissible purposes." To ensure compliance, CRAs must maintain reasonable procedures to ensure that such third party disclosures are made exclusively for permissible purposes. 15 U.S.C. § 1681e(a).

12. The FCRA defines "consumer report" broadly, as "any written, oral, or other communication of any information by a CRA bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title." 15 U.S.C. 1681a(d).

13. The FCRA also entitles the consumer to take an active role in the protection of his or her sensitive personal information, by giving the consumer a right to request "All information in the consumer's file at the time of the request." 15 U.S.C. § 1681g(a)(1). Through immediate review of the details of when, and for what purpose, a consumer's information has been disclosed to a third party, a consumer may better understand whether their identity has been stolen.

14. The FCRA also entitles consumers to actively protect their privacy rights in cases of suspected identity theft. Specifically, a consumer who believes he or she has been the victim of identity theft can submit a fraud alert to a consumer reporting agency. 15 § U.S.C. 1681c-1. The consumer can either request that the fraud alert be imposed for a 90-day period, or for an extended period of seven years. 15 U.S.C. § 1681c-1(a)-(b). In the event a consumer requests "extended" protection, a consumer reporting agency must remove the consumer from any list of third parties to whom the agency sends the consumer's information to extend firm offers of credit, and keep the consumer off of any such a list for five years, unless the consumer requests otherwise. 15 U.S.C. § 1681c-1(b)(1)(B). After being notified of a fraud alert, a CRA must send notification of the alert to the consumer reporting agencies which report information on a nationwide basis. 15 U.S.C. § 1681c-1(a)(1)(B); *see* 15 U.S.C. § 1681a(p).

15. After fraud notification, the FCRA provides the consumer additional rights to independently monitor their credit information to protect their privacy. Specifically, once notified of a consumer's fraud notification, a CRA must, within three days of the notification, provide the consumer with all of the disclosures required under 15 U.S.C. § 1681g. 15 U.S.C. §§ 1681c-1(a)(2), 1681c-1(b)(2). When a consumer requests that an "extended" fraud alert be placed on their files, the consumer is entitled to request two free disclosures under 15 U.S.C. § 1681g within the 12-month period following notification of a fraud alert. 15 U.S.C. § 1681c-1(b). Thus, through immediate review of the details of when, and for what purpose, a consumer's private information has been disclosed to a third party, a consumer may better understand whether their identity has been stolen. And through semi-annual review of their consumer disclosures in the case of an "extended" alert, a consumer can periodically check to determine whether efforts to

protect their identity after potential fraud have not been successful. Thus, the FCRA presupposes that consumers subject to potential fraud should be permitted the immediate opportunity to investigate the issues themselves and ascertain the extent of any suspected fraud.

16. Plaintiff, individually and on behalf of those similarly situated, brings this action to challenge the actions of Defendant in the protection and safekeeping of the Plaintiff's and class members' personal information, as well as to timely notify Plaintiff and class members of suspected fraud.

17. Defendant failed to properly safeguard the information of Plaintiffs and Class members, as required under 15 U.S.C. § 1681e(a).

18. Defendant's failure to properly safeguard the personal information of Plaintiffs and the class members is in violation of Iowa Code chapter 715C

19. Defendant's actions or omissions also constituted negligence.

GENERAL ALLEGATIONS

20. Equifax, a global corporation, "organizes, assimilates and analyzes data on more than 820 million consumers and more than 91 million businesses worldwide, and its database includes employee data contributed from more than 7,100 employers." (http://www.equifax.com/about-equifax/company-profile/ (September 11, 2017)).

21. The data Equifax stores includes Plaintiff's and class members' personal identifying information, such as names, full Social Security numbers, birth dates, addresses, driver's license numbers, and credit card numbers (collectively, "PII"). At all relevant times, Equifax knew or should have known that the PII it collected and stored is valuable, highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties.

22. Equifax, is engaged in the business of using consumers' PII to generate credit reports, which it sells to lenders and other entities. *See* Business, http://www.equifax.com/business/all-products (last visited Sept. 15, 2017).

23. Equifax is engaged in the business of selling decision analytic services and marketing services to lenders and other entities. *See id*.

24. Equifax also provides services directly to consumers by assisting consumers to access their credit history and score, assistance in managing their financial status, and helping consumers to protect themselves against fraud and identity theft. *See, e.g*., Personal, https://www.equifax.com/personal/ (last visited Sept. 15, 2017).

25. On July 29, 2017, Equifax discovered that one or more of its servers, which contained Plaintiff's sensitive personal information including Plaintiff's name, full Social Security number, birth date, address, and, upon belief, driver's license numbers and possibly one or more credit card numbers, had been breached or "hacked" by a still unknown third party. Such information constitutes a "consumer report" because it is information "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living." 15 U.S.C. 1681a(d).

26. Upon information and belief, when Equifax discovered this breach, Equifax began an internal investigation and contracted with an unidentified third-party cybersecurity firm to conduct a comprehensive forensic review to determine the scope of the hack including identifying the specific data impacted. As of the filing of this Complaint, that investigation remains ongoing and has yet been completed despite over six weeks elapsing since the initial breach.

27. After Equifax discovered the breach but before notifying Plaintiff, class members, and all other consumers, three (3) Equifax executives, including the Chief Financial Officer, John Gamble, sold shares of Equifax stock worth nearly $2 million. *See, e.g.*, Alina Selyukh, *Equifax Executives Sold Stock Days After Hack That Wasn't Disclosed For A Month*, NPR, Sept. 8, 2017, *available at* http://www.npr.org/sections/thetwo-way/2017/09/08/549434187/3-equifax-executives-sold-stock-days-after-hack-that-wasnt-disclosed-for-a-month

28. On September 7, 2017, major news outlets began reporting about the July 29, 2017 incident. (*See, e.g*, *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, Tara Siegel Bernard et al., NY TIMES, Sept. 7, 2017, *available at* https://www.nytimes.com/2017/09/07/business/equifaxcyberattack.html?hp&action=click&pgtype=Homepage&clickSource=story-heading&module=first-column-region&region=top news&WT.nav=top-news).

29. For Plaintiff, as with all potential class members, these news stories were the first time he had been informed that his information secured by Equifax had been compromised six (6) weeks earlier, and they now live in constant fear that their information has been compromised.

30. Equifax's decision to wait six (6) weeks after the alleged data breach before informing all consumers of the same was willful, or at least negligent. Further, by depriving Plaintiff and Class members information about the breach in a timely manner, Equifax subjected each consumer to a concrete informational injury, as these consumers were deprived of their opportunity to meaningfully consider and address issues related to the potential fraud, as well as to avail themselves of the remedies available under the

FCRA to prevent further dissemination of their private information, including but not limited to the potential remedies under 15 U.S.C. §§ 1681g, 1681c-1, and 1681c-2. 25.

31. Equifax has been subject to numerous allegations regarding data breaches in the past. (See, e.g., A Brief History of Equifax Security Fails, Thomas Fox-Brewster, FORBES, Sept. 8, 2017, *available at* https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#63dc4270677c). In light of Equifax's continual failure to ensure the integrity of its file storage systems in light of known defects to the same, Equifax willfully, or at least negligently, failed to enact reasonable procedures to ensure that consumer reports would only be provided for a permissible purpose. By failing to establish reasonable procedures to safeguard individual consumer's private information, Equifax deprived millions of consumers from a benefit conferred on them by Congress, which, now lost, cannot be reclaimed.

32. The harm to Plaintiff and class members was complete at the time the unauthorized breaches occurred, as the unauthorized disclosure and dissemination of private credit information causes harm in and of itself.

33. Plaintiff suffered actual injury including but not limited to damages to and diminution in the value of his PII – a form of intangible property that was entrusted to Equifax, and that was compromised in and as a result of the data breach

34. Plaintiff suffered additional actual injury, including but not limited to the costs associated with his attempt to limit the damage caused by Equifax, including the September 12, 2017, "freezing" of his credit with Equifax and the payment of fees to freeze his credit with the other credit bureaus, Experian and TransUnion. The "freeze" of Plaintiff's credit caused monetary damage to him and has restricted his ability to borrow money or conduct other credit transactions requiring a credit score.

35. While Equifax has offered one year of free identify theft protection to the affected consumers called "TrustedID Premier," this remedy is inadequate as the fallout from the data breach will certainly last longer than one year. Plaintiff and other similarly situated consumers will need to purchase identify theft protection after the expiration of this one-year service, creating a further monetary burden on Plaintiff and other similar consumers and a future monetary gain to Defendant.

36. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by their PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

37. Plaintiff and class members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

38. The Equifax Data Breach was a direct and proximate result of Equifax's failure to properly safeguard and protect Plaintiff and Class members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Equifax's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class members' PII to protect against reasonably foreseeable threats to the security or integrity of such information.

39. Equifax had the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

40. As a direct and proximate result of Equifax's wrongful actions and inaction and the resulting Data Breach, Plaintiff and class members have been placed at an

imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured. In all manners of life in this country, time has constantly been recognized as compensable, for many consumers it is the way they are compensated, and even if retired from the work force, consumers should be free of having to deal with the consequences of a credit reporting agency's slippage, as is the case here.

41. Equifax's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff and class members' PII, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation.

CLASS ALLEGATIONS

42. Plaintiff brings this action on behalf of a nationwide class of all similarly situated individuals (Class), defined as: "all persons in the United States for whom Equifax stored private, personal information that was released as a result of the data breach."

> Excluded from the Class are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter

finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

43. Plaintiff also brings this action on behalf of a subclass of all similarly situated individuals in Iowa (Subclass), defined as: "all persons in Iowa for whom Equifax stored private personal information that was released as a result of the data breach."

Excluded from the Subclass are: (1) Defendant, Defendant's agents, subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parents have a controlling interest, and those entities' current and former employees, officers, and directors; (2) the Judge to whom this case is assigned and the Judge's immediate family; (3) any person who executes and files a timely request for exclusion from the Class; (4) any persons who have had their claims in this matter finally adjudicated and/or otherwise released; and (5) the legal representatives, successors and assigns of any such excluded person.

44. At this time Plaintiff does not know the size of the Class because the information is exclusively in the possession of the Defendant, but Plaintiff believes that the potential number of Class members are so numerous that joinder would be impracticable. It has been reported that the Class could consist of over 100 million people. The number of Class members can be determined through discovery, particularly investigation of Equifax's internal records.

45. All members of the Class have been subject to and affected by a uniform course of conduct in that all Class members' personal information was compromised during the data breach. These are questions of law and fact common to the proposed Class that predominate over any individual questions. The questions common to all Class members include, but are not limited to

a. Whether Defendant had implemented reasonable procedures to ensure that all third parties who accessed Plaintiffs' and Class members' private credit information did so for a permissible purpose;

b. Whether Defendant failed to notify consumers of the data breach within a reasonable period of time;

c. Whether Defendant failed to block the reporting of information on consumers' files that were the result of the data breach;

d. Whether Plaintiffs and Class members suffered damages as a result of Defendant's failure to comply with FCRA based on the improper dissemination of their credit information as a result of the data breach;

e. Whether Plaintiff and Class members are entitled to statutory damages; and

f. Whether Plaintiff and Class members are entitled to punitive damages.

46. Plaintiffs' claims are typical of the class, as Plaintiffs' personal information was compromised during the data breach. All claims are based on the same legal and factual issues.

47. Plaintiffs will adequately represent the interests of the class and do not have an adverse interest to the class. If individual class members prosecuted separate actions it may create a risk of inconsistent or varying judgments that would establish incompatible standards of conduct. A class action is the superior method for the quick and efficient adjudication of this controversy.

COUNT I: VIOLATION OF 15 U.S.C. 1681, *et seq*.

48. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

49. This Count is brought on behalf of the nationwide Class.

50. Based upon Equifax's failure to have reasonable procedures in place, Plaintiff's private information was compromised, and none of the Plaintiffs or Class members received notice of the data breach, except through the media, approximately six

(6) weeks after the breach occurred.

51. As a result of each and every willful violation of FCRA, Plaintiffs and Class members are entitled to: actual damages, pursuant to 15 U.S.C. 1681n(a)(1); statutory damages, pursuant to 15 U.S.C. 1681n(a)(1); punitive damages, as this Court may allow, pursuant to 15 U.S.C. 1681n(a)(2); and reasonable attorneys' fees and costs pursuant to 15 U.S.C. 1681n(a)(3). As a result of each and every negligent non-compliance of the FCRA, Plaintiffs and Class members are also entitled to actual damages, pursuant to 15 U.S.C. 16810(a)(1); and reasonable attorney's fees and costs pursuant to 15 U.S.C. 16810(a)(2) from Defendant.

COUNT II: VIOLATION OF Iowa Code Chapter 715C, *et seq*.

52. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

53. This Count is brought on behalf of the Iowa Subclass.

54. At all relevant times there was in full force and effect Iowa Code chapter 715C, *et seq*., Personal Information Security Breach Protection.

55. Iowa Code section 715C.1(1) defines "consumer" as "an individual who is a resident of this state."

56. A "[c]onsumer reporting agency" has the same definition as found in 15 U.S.C. § 1681a.

57. Iowa Code section 715C.1(1) defines "breach of security" as:

> an unauthorized acquisition of personal information maintained in computerized form by a person that compromises the security, confidentiality, or integrity of the personal information. "Breach of security" also means unauthorized acquisition of personal information maintained by a person in any medium, including on paper, that was transferred by the person to that medium from computerized form and that compromises the security, confidentiality, or integrity of the personal information.

58. Iowa Code section 715C.2(1) requires a "person who owns or licenses computerized data that includes a consumer's person information" that was subject to a security breach to give "expeditious" notification of the breach to the consumer.

59. Based upon Equifax's failure to have reasonable procedures in place, Plaintiff's private information was compromised, and none of the Plaintiffs or Iowa Class members received notice of the breach of security in the "most expeditious manner possible," except through the media, approximately six (6) weeks after the breach occurred. *See* Iowa Code § 715C.2(1).

60. Upon information and belief, none of the exclusions found in Iowa Code section 715C.2(7) are applicable to Defendant.

61. Plaintiff seeks any "rights and remedies available under the law," stemming from Defendant's violation of Iowa Code chapter 715C. *Id.* § 715C.2(9)(b).

COUNT IV: NEGLIGENCE

62. Plaintiff incorporates by reference as if fully set forth herein the allegations contained in the preceding paragraphs of this Complaint.

63. Upon accepting and storing the PII of Plaintiff and Class Members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Equifax knew that the PII was private and confidential and should be protected as private and confidential.

64. Equifax owed a duty of care not to subject Plaintiff, along with his PII, and Class members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

65. Equifax owed numerous duties to Plaintiff and to members of the Class, including the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. To protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

66. Equifax knew, or should have known, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the importance of adequate security.

67. Equifax knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff and class Members' PII.

68. Equifax's own conduct also created a foreseeable risk of harm to Plaintiff and Class members and their PII. Equifax's misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

69. Equifax also had independent duties under state and federal laws that required Equifax to reasonably safeguard Plaintiff's and Class members' Personal Information and promptly notify them about the data breach.

70. Equifax breached its duties to Plaintiff and Class members in numerous ways, including:

a. By failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiff and Class members;

b. By creating a foreseeable risk of harm through the misconduct previously described;

c. By failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiff's and Class members' PII both before and after learning of the Data Breach;

d. By failing to comply with the minimum industry data security standards during the period of the Data Breach; and

e. By failing to timely and accurately disclose that Plaintiff's and Class members' PII had been improperly acquired or accessed.

71. Through Equifax's acts and omissions described in this Complaint, including Equifax's failure to provide adequate security and its failure to protect PII of Plaintiff and Class members from being foreseeably captured, accessed, disseminated, stolen and misused, Equifax unlawfully breached its duty to use reasonable care to adequately protect and secure PII of Plaintiff and Class members during the time it was within Equifax possession or control.

72. Further, through its failure to provide timely and clear notification of the Data Breach to consumers, Equifax prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their financial data and bank accounts.

73. Upon information and belief, Equifax improperly and inadequately safeguarded PII of Plaintiff and Class Members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive PII of Plaintiff and Class members as

described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiff and Class members.

74. Equifax's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiff and Class members; and failing to provide Plaintiff and Class members with timely and sufficient notice that their sensitive PII had been compromised.

75. Neither Plaintiff nor the other Class members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint. As a direct result of Equifax's conduct, Plaintiff and the Class suffered damages including, but not limited to: damages arising from the unauthorized charges on their debit or credit cards or on cards that were fraudulently obtained through the use of the PII of Plaintiff and Class Members; damages arising from Plaintiff's inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charges and foregone cash back rewards; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by expending monies to place "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports and damages from identity theft, which may take months if not years to discover and detect, given the far-reaching, adverse and detrimental consequences of identity theft and loss of privacy. The nature of

other forms of economic damage and injury may take years to detect, and the potential scope can only be assessed after a thorough investigation of the facts and events surrounding the theft mentioned above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, James A. Cederdahl, prays for judgment against Defendant, Equifax Information Services, LLC, and the following remedies:

a) For an award of actual damages against Defendant for all allegations contained in the Counts above;

b) For an award of punitive damages against Defendant for the allegations contained in Count One as this Court may allow pursuant to 15 U.S.C. 1681n(a)(2)

c) For an award of the costs of litigation and reasonable attorneys' fees pursuant to 15 U.S.C. 1681n(a)(3) and 15 U.S.C. 1681(o)(1)(1) against Defendant for each incident of noncompliance of FCRA alleged in Count One and under Iowa Code chapter 715C as alleged in Count Two;

d) For all other relief this Court may deem just and proper**.**

JURY DEMAND

Plaintiff hereby demands a trial by jury.

Respectfully Submitted, By:

PATTERSON LAW FIRM, L.L.P.
505 Fifth Avenue, Suite 729
Des Moines, IA 50309
Phone: (515) 283-2147
FAX: (515) 283-1002
E-mail: jmiller@pattersonfirm.com
E-mail : jcook@pattersonfirm.com

By: */s/ Jason W. Miller*_____
Jason W. Miller

By: */s/ Jeffrey J. Cook*_____
Jeffrey J. Cook

ATTORNEYS FOR PLAINTIFF